UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23669 7590 07/29/2008

HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
ZEE, EDWARD	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/29/2008

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,435	04/16/2004	G. Glenn Henry	CNTR.2075	9993

TITLE OF INVENTION: MICROPROCESSOR APPARATUS AND METHOD FOR PROVIDING CONFIGURABLE CRYPTOGRAPHIC BLOCK CIPHER ROUND RESULTS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1440	$300	$0	$1740	10/29/2008

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23669 7590 07/29/2008

HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,435	04/16/2004	G. Glenn Henry	CNTR.2075	9993

TITLE OF INVENTION: MICROPROCESSOR APPARATUS AND METHOD FOR PROVIDING CONFIGURABLE CRYPTOGRAPHIC BLOCK CIPHER ROUND RESULTS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1440	$300	$0	$1740	10/29/2008

EXAMINER	ART UNIT	CLASS-SUBCLASS
ZEE, EDWARD	2135	713-190000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,435	04/16/2004	G. Glenn Henry	CNTR.2075	9993

23669 7590 07/29/2008

HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
ZEE, EDWARD	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/29/2008

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 715 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 715 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	10/826,435	HENRY ET AL.	
	Examiner	Art Unit	
	EDWARD ZEE	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendments filed on 03/07/08 and the telephonic interview conducted on 06/16/08*.

2. ☒ The allowed claim(s) is/are *1-16, 19, 21-25 and 28-30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. As per MPEP 713.04, a separate interview summary form is not provided as the substance of the interview has been summarized herein.

Authorization for this examiner's amendment was given in a telephone interview with Richard K. Huffman (No. 41,082) on June 16th, 2008.

The application has been amended as follows:

Please replace the claims as follows:

1. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a microprocessor;

a control word, configured to prescribe that an intermediate result be generated during execution of one of the cryptographic operations, wherein said control word is stored in memory, and wherein a memory location of said control word is prescribed by contents of a register that is referenced by a single atomic cryptographic instruction;

fetch logic, disposed within [[a]]said microprocessor, configured to receive [[a]]said single atomic cryptographic instruction as part of an instruction flow executing on said microprocessor, wherein said single atomic cryptographic instruction prescribes said one of the cryptographic operations, and wherein said single atomic cryptographic instruction [[prescribes]] references said control word;

translation logic, coupled to said fetch logic and disposed within said microprocessor, configured to translate said single atomic cryptographic instruction into a sequence of micro instructions that directs said microprocessor to perform said one of the cryptographic operations; and

execution logic, disposed within said microprocessor and operatively coupled to said single atomic cryptographic instruction, configured to execute said one of the cryptographic operations, and configured to generate said intermediate result, wherein said execution logic comprises:

a cryptography unit, configured to execute a plurality of cryptographic rounds on each of one or more input text blocks to generate a corresponding each of one or more output text blocks, wherein said plurality of cryptographic rounds are prescribed by a round count field within ~~a control word that is provided to said cryptography unit~~said control word.

2. (Original) The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

an encryption operation, said encryption operation comprising encryption of one or more plaintext blocks to generate a corresponding one or more ciphertext blocks.

3. (Original) The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

a decryption operation, said decryption operation comprising decryption of one or more ciphertext blocks to generate a corresponding one or more plaintext blocks.

4. (Currently Amended) The apparatus as recited in claim 1, wherein said execution logic is configured to interpret an intermediate result field within [[a]]said control word which is referenced by said single atomic cryptographic instruction.

5. (Original) The apparatus as recited in claim 4, wherein said intermediate result field directs said execution logic to generate said intermediate result.

6. (Original) The apparatus as recited in claim 4, wherein said intermediate result field directs said execution logic to generate a normal result.

7. (Currently Amended) The apparatus as recited in claim 1, wherein said execution logic is configured to interpret a round count field within [[a]]said control word which is referenced by said single atomic cryptographic instruction.

8. (Original) The apparatus as recited in claim 7, wherein the value of said round count field prescribes a number of cipher rounds to be performed on an input block during execution of said one of the cryptographic operations.

9. (Original) The apparatus as recited in claim 1, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

10. (Original) The apparatus as recited in claim 1, wherein said single atomic cryptographic instruction is prescribed according to the instruction format for execution on an x86-compatible microprocessor.

11. (Original) The apparatus as recited in claim 1, wherein said single atomic cryptographic instruction implicitly references one or more registers within said microprocessor.

12. (Original) The apparatus as recited in claim 11, wherein said one or more registers comprises: a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of one or more input text blocks upon which said one of the cryptographic operations is to be accomplished.

13. (Original) The apparatus as recited in claim 11, wherein said one or more registers comprises: a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding one or more output text blocks, said corresponding one or more output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon one or more input text blocks.

14. (Original) The apparatus as recited in claim 11, wherein said one or more registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within one or more input text blocks.

15. (Original) The apparatus as recited in claim 11, wherein said one or more registers comprises: a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

16. (Original) The apparatus as recited in claim 11, wherein said one or more registers comprises: a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising a initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations.

17. (Cancelled)

18. (Cancelled)

19. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a microprocessor;

a control word, configured to prescribe that an intermediate result be generated during execution of one of the cryptographic operations, wherein said control word is stored in memory, and wherein a memory location of said control word is prescribed by contents of a register that is referenced by a single atomic cryptographic instruction; and

a cryptography unit disposed within execution logic in [[a]]said microprocessor, configured to execute said one of the cryptographic operations responsive to receipt of [[a]]said single atomic cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said single atomic cryptographic instruction is fetched from memory by fetch logic in said

microprocessor, ~~and wherein said single atomic cryptographic instruction also references said control word~~and wherein translation logic in said microprocessor translates said single atomic cryptographic instruction into a sequence of micro instructions that directs said microprocessor to perform said one of the cryptographic operations.

20. (Cancelled)

21. (Original) The apparatus as recited in claim 19, wherein said cryptography unit executes said one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

22. (Original) The apparatus as recited in claim 19, wherein said cryptography unit interprets an intermediate result field within said control word to determine whether to generate a normal result or said intermediate result.

23. (Original) The apparatus as recited in claim 19, wherein said cryptography unit interprets a round count field within said control word to determine how many block cipher rounds to execute on a block of input text during execution of said one of the cryptographic operations.

24. (Previously Presented) The apparatus as recited in claim 19, wherein said single atomic cryptographic instruction is prescribed according to the instruction format for execution on an x86-compatible microprocessor.

25. (Currently Amended) A method for performing cryptographic operations, comprising:

via fetch logic within a microprocessor, fetching a single atomic cryptographic instruction from memory prescribing ~~that an intermediate result be generated during execution of~~ one of a plurality of cryptographic operations;

via a first field within a control word that is referenced by the single atomic cryptographic instruction, specifying whether a normal result or the intermediate result is to be generated during execution of the one of a plurality of cryptographic operations; and

loading the control word from memory;

via translation logic disposed within the microprocessor, translating the single atomic cryptographic instruction into a sequence of micro instructions that direct the microprocessor to perform the one of the plurality of cryptographic operations, and via a cryptography unit disposed within execution logic in the microprocessor, generating the intermediate result when executing the one of the cryptographic operations.

26. (Cancelled)

27. (Cancelled)

28. (Original) The method as recited in claim 25, said receiving comprises:

executing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

29. (Previously Presented) The apparatus as recited in claim 22, wherein said prescribing comprises:

providing the single atomic cryptographic instruction according to the instruction format for execution on an x86-compatible microprocessor.

30. (Currently Amended) The method as recited in claim 25, wherein said prescribing comprises:

via a second field within [[a]]the control word that is referenced by the single atomic cryptographic instruction, specifying how many cipher rounds are to be executed during execution of the one of the cryptographic operations on a block of input text.

3. The following is an examiner's statement of reasons for allowance: the arguments filed on March 7th, 2008 have been fully considered and are persuasive, in particular the remarks found on pages 17 to 20. Therefore, Claims 1-16, 19, 21-25 and 28-30 are allowable over the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
June 16, 2008
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135